SC402- Introduction to Cryptography
Assignment 2

1. Suppose we consider a random throw of a pair of dice. Let X be the random variable defined on the set $X = \{2, \ldots, 12\}$, obtained by considering the sum of two dice. Further, suppose that Y is a random variable which takes on the value D if the two dice are the same (i.e., if we throw "doubles"), and the value N, otherwise. Determine all the joint and conditional probabilities, $\mathbf{Pr}[x, y]$, $\mathbf{Pr}[x|y]$, and $\mathbf{Pr}[y|x]$, where $x \in \{2, \ldots, 12\}$ and $y \in \{D, N\}$.

2. Let $\mathcal{P} = \{a, b\}$ and let $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$. Let $\mathcal{C} = \{1, 2, 3, 4, 5\}$, and suppose the encryption functions are represented by the following encryption matrix:

	a	b
K_1	1	2
K_2	2	3
K_3	3	1
K_4	4	5
K_5	5	4

   Now choose two positive real numbers α and β such that $\alpha + \beta = 1$, and define $\mathbf{Pr}[K_1] = \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \alpha/3$ and $\mathbf{Pr}[K_4] = \mathbf{Pr}[K_5] = \beta/2$.

   Prove that this cryptosystem achieves perfect secrecy.

3. (a) Prove that the *Affine Cipher* achieves perfect secrecy if every key is used with equal probability 1/312.

   (b) More generally, suppose we are given a probability distribution on the set

$$\{a \in \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

   Suppose that every key (a, b) for the *Affine Cipher* is used with probability $\mathbf{Pr}[a]/26$. Prove that the *Affine Cipher* achieves perfect secrecy when this probability distribution is defined on the keyspace.

4. Suppose that $\mathbf{S}$ is a random variable representing the sum of a pair of dice. Compute $H(\mathbf{S})$.

5. Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Given that keys are chosen equiprobably, and the plaintext probability distribution is $\mathbf{Pr}[a] = 1/2$, $\mathbf{Pr}[b] = 1/3$, $\mathbf{Pr}[c] = 1/6$, compute $H(\mathbf{P})$, $H(\mathbf{C})$, $H(\mathbf{K})$, $H(\mathbf{K}|\mathbf{C})$, and $H(\mathbf{P}|\mathbf{C})$.